IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application of:	Date: November 27, 2006
Philip Lee CHILDS et al.	Confirmation No: 7874
Serial No: 10/063,402	Group Art Unit: 2145
Filed: April 18, 2002	Examiner: Ajay M. Bhatia

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF ON APPEAL

Pursuant to 37 CFR 1.193(b)(1), Applicant responds to the Examiner's Answer mailed October 25, 2006, as follows:

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the Appeal Brief.

(2) Related Appeals and Interferences

A statement identifying the related appeals and interferences is contained in the Appeal Brief.

(3) Status of Claims

A statement identifying the status of the claims is contained in the Appeal Brief.

(4) Status of Amendments

A statement identifying the status of amendments is contained in the Appeal Brief.

(5) Summary of Claimed Subject Matter

A summary of the claimed subject matter is contained in the Appeal Brief.

(6) Grounds of Rejection to be Reviewed on Appeal

A statement identifying the grounds of rejection to be reviewed on appeal is contained in the Appeal Brief.

(7) Response to Examiner's Answer

On page 11 of the Office Communication mailed October 25, 2006, the Examiner asserts that "Batten-Carew teaches 'isolating administrative access to a plurality of client system[s] in a computer network via a data center' in order of Batten-Carew administrator 18 in figure 1 to communicate with end-users 36, 38, 40 those communication must travel through the serving entity 12".

While such may be true for communications between the administrative entity 18 and the end-users 36, 38, 40, the administrative entity 18 can directly provide an administrative request to end-users 28, 30, 32, 34 (see col. 7 ll. 8-15), and, therefore, Batten-Carew fails to disclose isolating administrative access to a plurality of client system[s] in a computer network via a data center (i.e., the serving entity 12).

Furthermore, in rejecting claim 5, the Examiner cites several portions of Batten-Carew – specifically, col. 3, lines 41-61, col. 4, lines 9-21, col. 4, lines 32-44, col. 4 lines 45-67, col. 5, lines 4-11, col. 7 line 65 – col. 8, line 14, and col. 6, lines 9-22 - as

disclosing issuing a trusted message from a data center to at least one managed client when the authenticated administrative system has permission to perform a service command. Applicant respectfully disagrees.

In the cited portions above, Batten-Carew discloses only the serving entity 12 verifying a signature of the administrative entity 18, and the administrative entity 18 verifying a signature of the serving entity 12 (see FIG. 1) – and not the issuance of a trusted message from a data center (serving entity) to a managed client (end-user).

While Batten-Carew does disclose that the end-users 22-40 (or managed clients) are equipped with encryption software (see col. 3, lines 11-14), Batten-Carew discloses that the end-users transmits encrypted messages only to other end-users (col. 3, lines 14-17). Batten-Carew clearly fails to disclose that the serving entity transmits encrypted messages to an end-user – i.e., Batten-Carew fails to disclose that the administrative requests provided to an end-user by the serving entity is an encrypted message.

Conclusion

Neither Batten-Carew and Davis discloses isolating administrative access to a plurality of client systems in a computer network via a data center for those reasons stated in the Appeal Brief. Batten-Carew and Davis also fail to disclose issuing a trusted message from the data center to at least one managed client system when the authenticated administrator system does have authorization to perform the service command, as required by the claims, for those reasons discussed above. Applicant, therefore, respectfully submits that the pending claims 5-14 and 19-20 are not properly rejected under § 102 or § 103.

Please charge any fee that may be necessary for the continued pendency of this application to Deposit Account No. 50-3533 (Lenovo, Inc.).

Respectfully submitted,
SAWYER LAW GROUP LLP

November 28, 2006
Date

/KELVIN M. VIVIAN/
Kelvin M. Vivian
Attorney for Applicant
Reg. No. 53,727
(650) 475-1448

Appendix of Claims

1-4. (Cancelled)

5. (Previously Presented) A method for autonomic administration isolation for a secure remote management in a computer network, the method comprising:

(a) isolating administrative access to a plurality of client systems in a computer network via a data center; and

(b) utilizing the data center to control remote initiation of services in the plurality of client systems by an administrator system, the administrator system being a computer through which an administrator manages at least one of the plurality of client systems, wherein utilizing the data center further includes,

(b1) verifying authentication of the administrator system by the data center;

(b2) receiving a service command from the authenticated administrator system in the data center;

(b3) determining in the data center whether the authenticated administrator system has authorization to perform the service command in the at least one managed client system; and

(b4) issuing a trusted message from the data center to the at least one managed client system when the authenticated administrator system does have authorization to perform the service command.

6. (Previously Presented) The method of claim 5, further comprising (c) validating and decrypting the trusted message in the at least one managed client system to perform the service command.

7. (Previously Presented) An autonomic system for selective administration isolation for secure remote management in a computer network, the system comprising:

a network;

at least one administrator system coupled to the network, the at least one administrator system operable to transmit one or more service commands for managing one or more client systems;

at least one client system coupled to the network; and

a data center coupled to the at least one administrator system and to the at least one client system via the network, the data center for:

isolating administrative access to the at least one client system and controlling remote initiation of services in the at least one client system by the at least one administrator system including,

receiving a service command from the at least one administrator system, the service command having been issued after authentication of a first user associated with the at least one administrator system; and

issuing a trusted message to remotely control the at least one client system according to the service command, the trusted message having been issued after authentication of a second user associated with the data center, wherein the first user is different from the second user.

8. (Original) The system of claim 7, wherein the at least one administrator system includes authentication capabilities via an embedded security chip for unique system identification and biometric identification for unique user identification.

9. (Previously Presented) The system of claim 7, wherein the data center verifies authentication of the at least one administrator system.

10. (Previously Presented) The system of claim 7, wherein the authentication of a second user associated with the data center includes a user ID and password known only to the data center and an agent running on the at least one client system.

11. (Previously Presented) The system of claim 9, wherein the data center determines whether the authenticated administrator system has authorization to perform the service command in the at least one client system prior to issuing the trusted message to the at least one client system.

12. (Previously Presented) The system of claim 11, wherein the data center issues a trusted message to the at least one client system when the authenticated administrator system does have authorization to perform the service command.

13. (Previously Presented) The system of claim 12, wherein the at least one client system validates and decrypts the trusted message to perform the service command.

14. (Original) The system of claim 9, wherein the network further comprises a world wide web network.

15-18. (Cancelled)

19. (Previously Presented) A computer readable medium containing program instructions tangibly stored thereon for autonomic administration isolation in a computer network for a secure remote management, the program instructions for:

(a) isolating administrative access to a plurality of client systems in a computer network via a data center; and

(b) controlling remote initiation of services in the plurality of client systems by an administrator system via the data center, the administrator system being a computer through which an administrator manages at least one of the plurality of client systems, wherein controlling remote initiation of services via the data center includes,

(b1) verifying authentication of the administrator system by the data center;

(b2) receiving a service command from the authenticated administrator system in the data center;

(b3) determining in the data center whether the authenticated administrator system has authorization to perform the service command in the at least one managed client system; and

(b4) issuing a trusted message from the data center to the at least one managed client system when the authenticated administrator system does have authorization to perform the service command.

20. (Previously Presented) The computer readable medium of claim 19, further comprising (c) validating and decrypting the trusted message in the at least one managed client system to perform the service command.

21-23. (Cancelled)

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None